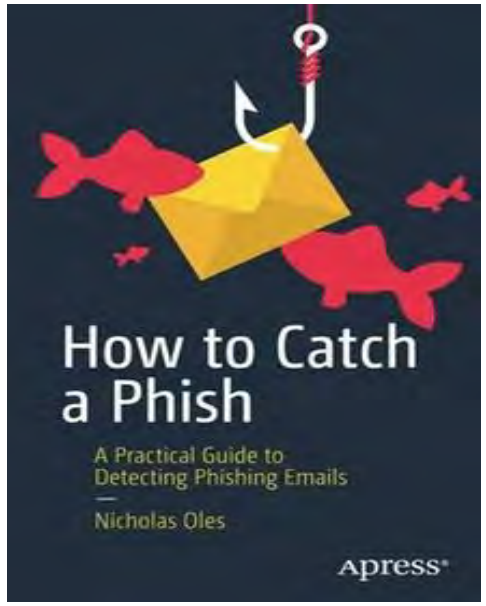
entoo SECURITY

Midwest to the Middle East: Learn to Catch Phish from a Special Ops Veteran and Phisherman

Agenda

- Introduction
- Phishing Overview
- How to Scan an Email
  - Sender/Recipient Verification
  - Greetings
  - Links and Attachments
  - Tools to Use
  - Handling and Reporting
- Cool Phish in the Wild

Who Am I?



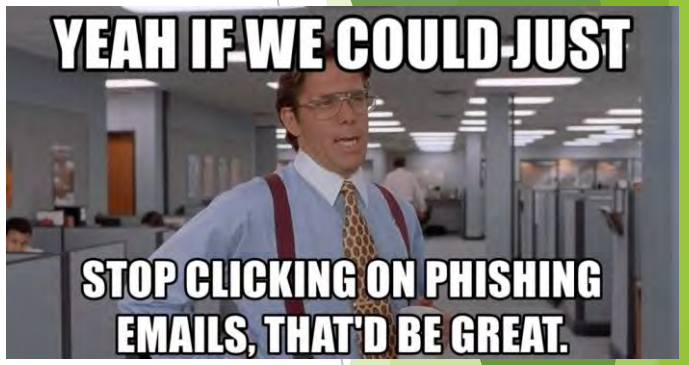
- 15 years in IT/Cybersecurity
- Military, government, civilian roles
- Published author and speaker
- Responded to thousands of email and security incidents
- Special Operations Advisor and veteran
- BS in Accounting MS in Cybersecurity
- 7 industry certifications
- 1000's of hours of formalized government and private sector training

What is Phishing?!

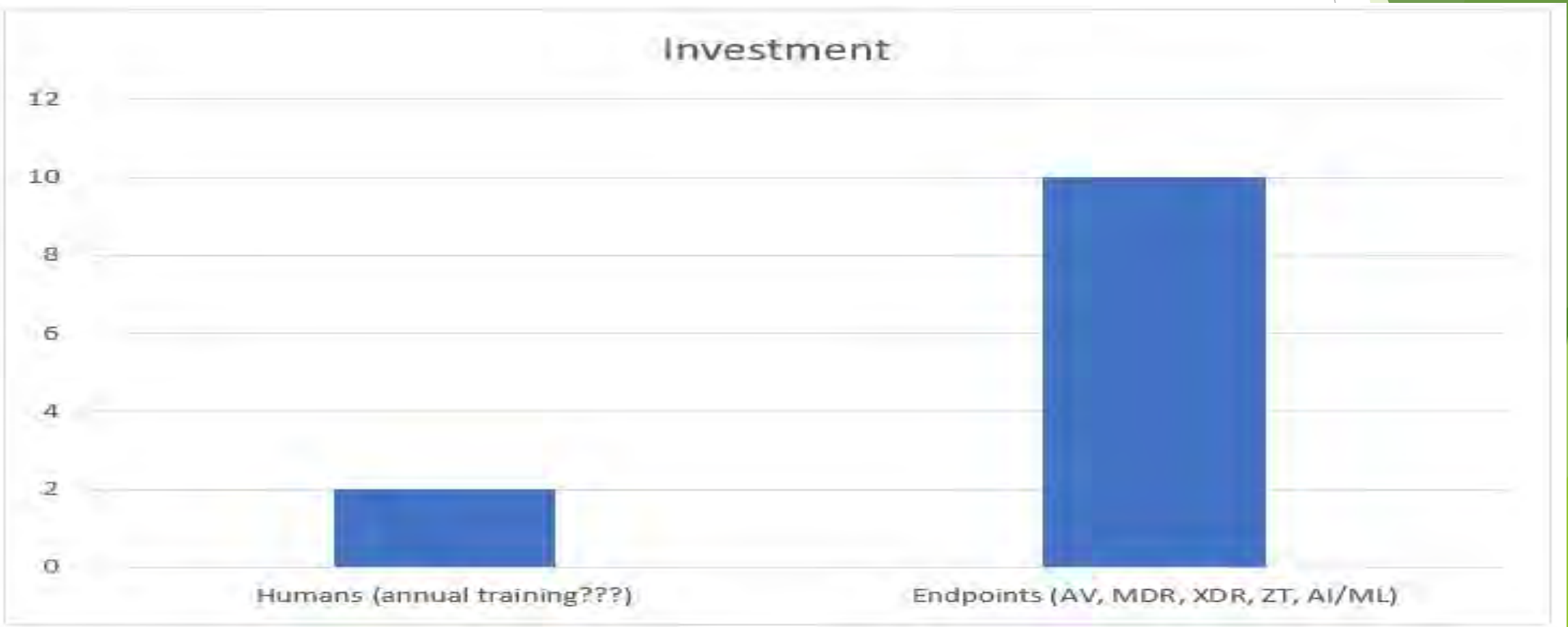
- **Threat actor uses technology to deceive an individual to take a specific action.**
  - **Multiple social engineering techniques to get you, a human, to:**
    - **Click a link**
    - **Provide sensitive information**
    - **Interacting with an attachment**

Phishing Why?

- 91% of successful data breaches start with a phishing attack. (Verizon)
- Google blocks over 100 million phishing emails a day.
- Phishing works, attackers aren't stopping.
- Training videos and simulated phishing attacks aren't good enough, if they were this wouldn't be a problem.
- Phishing simulations typically yield 2-8% click rates.

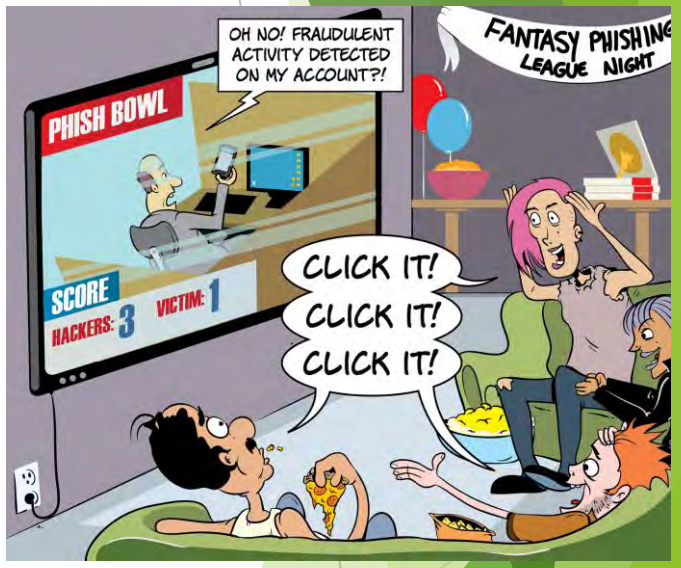


People vs Technologies



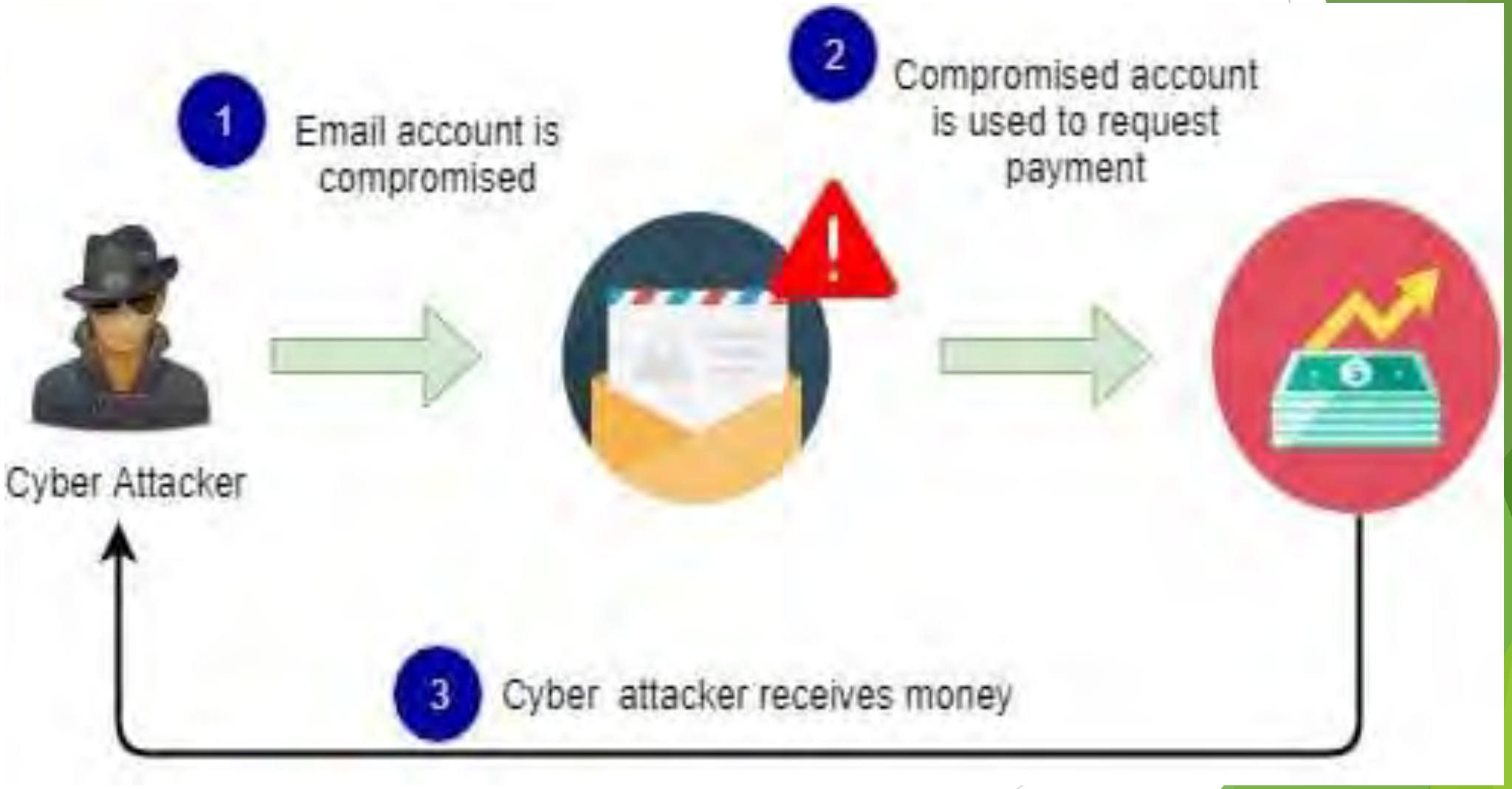
Phishing Impacts

- Unnecessary training, headaches, loss of funds.
- Criminals make money, nation states fund things (North Korea).
- The average cost of a data breach caused by phishing reached $4.88 million in 2024.
- Business Email Compromise (BEC) can crush a company. Insert tire story.



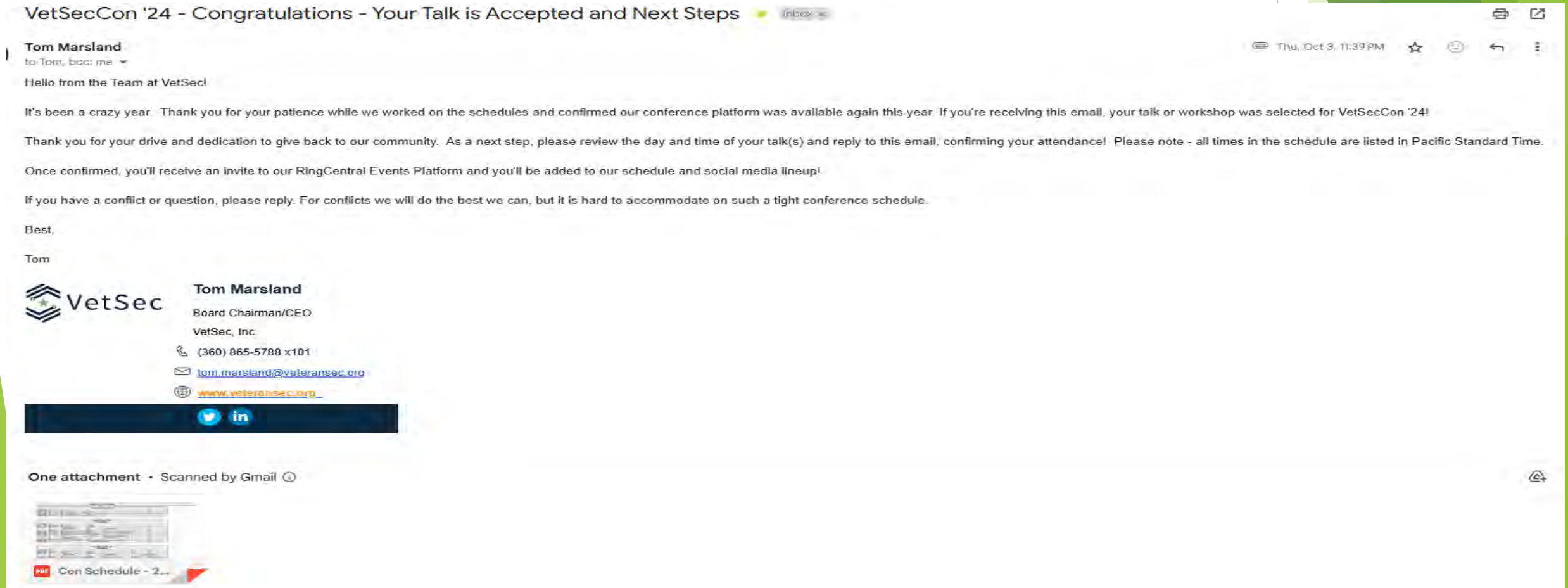
What type of Techniques?!

Business Email Compromise



Where to Start?

- Brief Scan of the email, step by step.



VetSecCon '24 – Congratulations – Your Talk is Accepted and Next Steps Inbox

Tom Marsland
to Tom, bcc: me

Thu, Oct 3, 11:39 PM

Hello from the Team at VetSec!

It's been a crazy year. Thank you for your patience while we worked on the schedules and confirmed our conference platform was available again this year. If you're receiving this email, your talk or workshop was selected for VetSecCon '24!

Thank you for your drive and dedication to give back to our community. As a next step, please review the day and time of your talk(s) and reply to this email, confirming your attendance! Please note - all times in the schedule are listed in Pacific Standard Time.

Once confirmed, you'll receive an invite to our RingCentral Events Platform and you'll be added to our schedule and social media lineup!

If you have a conflict or question, please reply. For conflicts we will do the best we can, but it is hard to accommodate on such a tight conference schedule.

Best,

Tom

VetSec

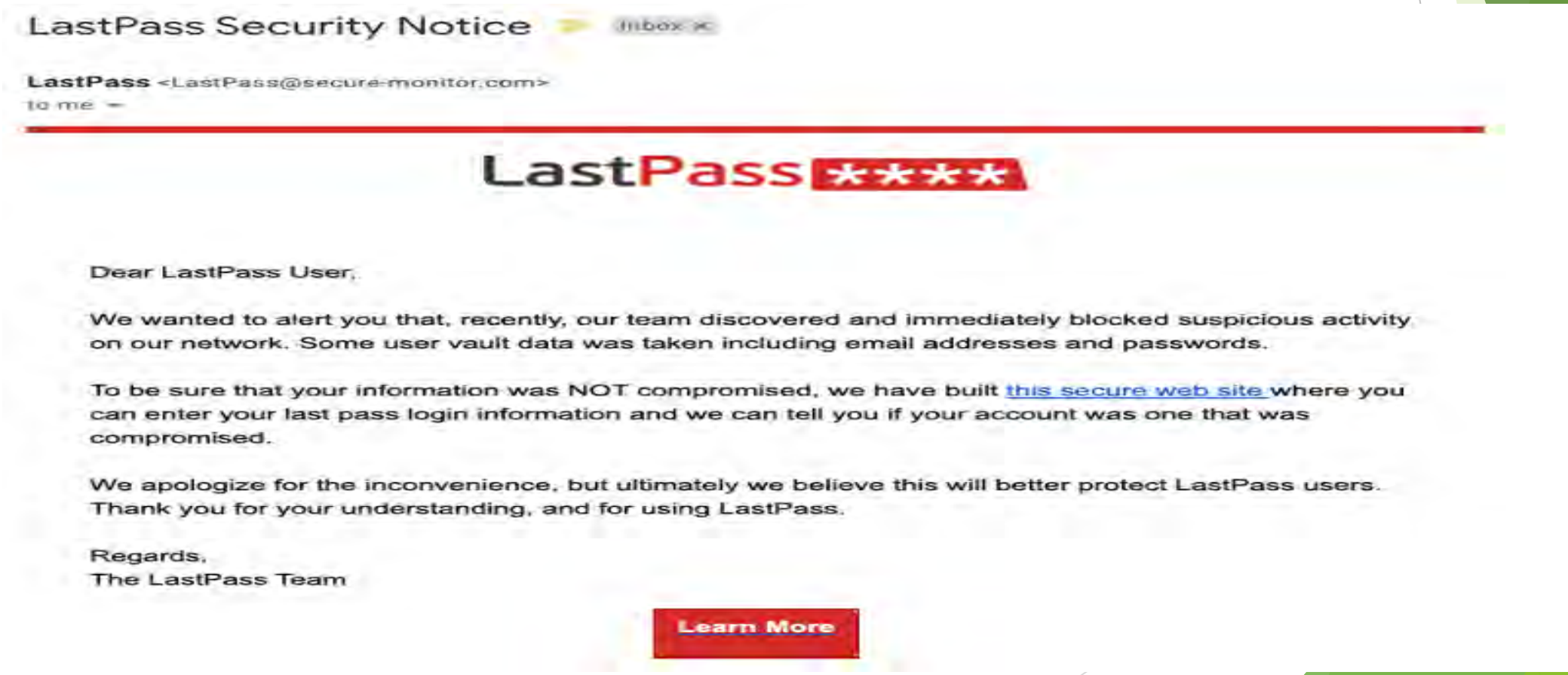
Tom Marsland
Board Chairman/CEO
VetSec, Inc.
(360) 865-5788 x101
tom.marsland@veteransec.org
www.veteransec.org

One attachment • Scanned by Gmail

Con Schedule - 2...

Sender/Recipient Address

- Scanning an email from top to bottom, starting with the sender and recipient addresses. What do you see?



LastPass Security Notice Inbox x

LastPass <LastPass@secure-monitor.com>
to me

LastPass ****

Dear LastPass User,

We wanted to alert you that, recently, our team discovered and immediately blocked suspicious activity on our network. Some user vault data was taken including email addresses and passwords.

To be sure that your information was NOT compromised, we have built this secure web site where you can enter your last pass login information and we can tell you if your account was one that was compromised.

We apologize for the inconvenience, but ultimately we believe this will better protect LastPass users. Thank you for your understanding, and for using LastPass.

Regards,
The LastPass Team

Learn More

Impersonation Using Sender Address

Display Name

Domain

<onlinebanking@e.chase.com>

Subdomain

Top Level Domain

Thu 10/29/2020 2:48 AM

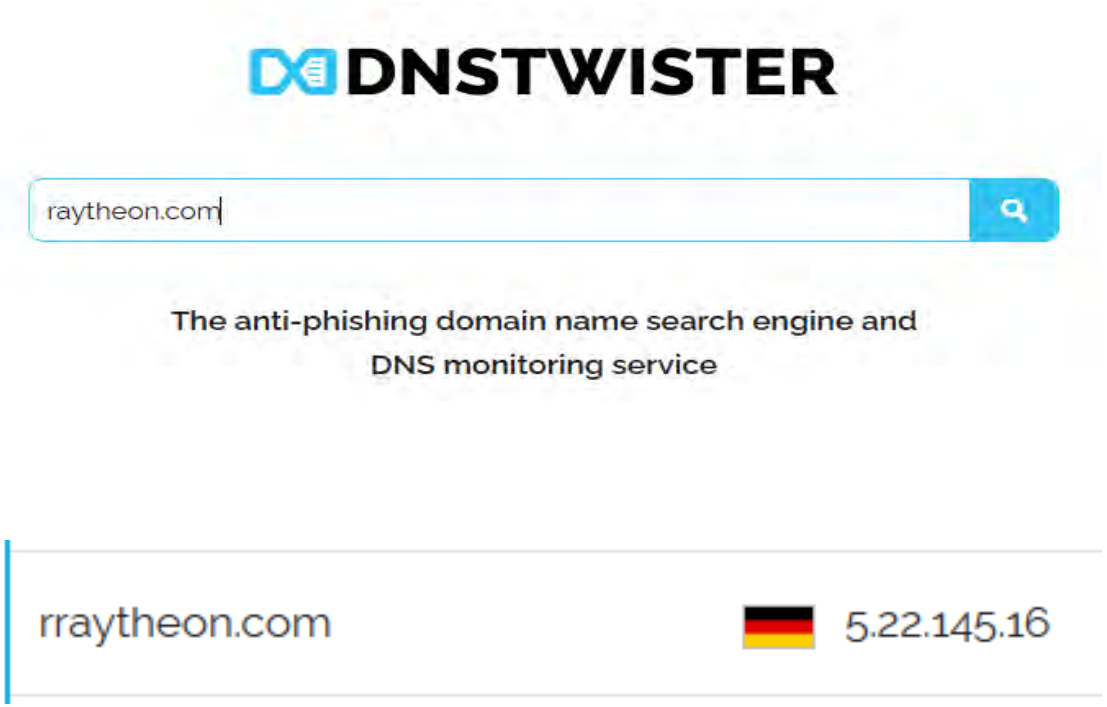
Chase Fraud Alert <onlinebanking@e.chase.com>

Action Needed: Activity On Your Chase Debit or ATM Card on 10/28/2020 [MALD ID: 5324223]

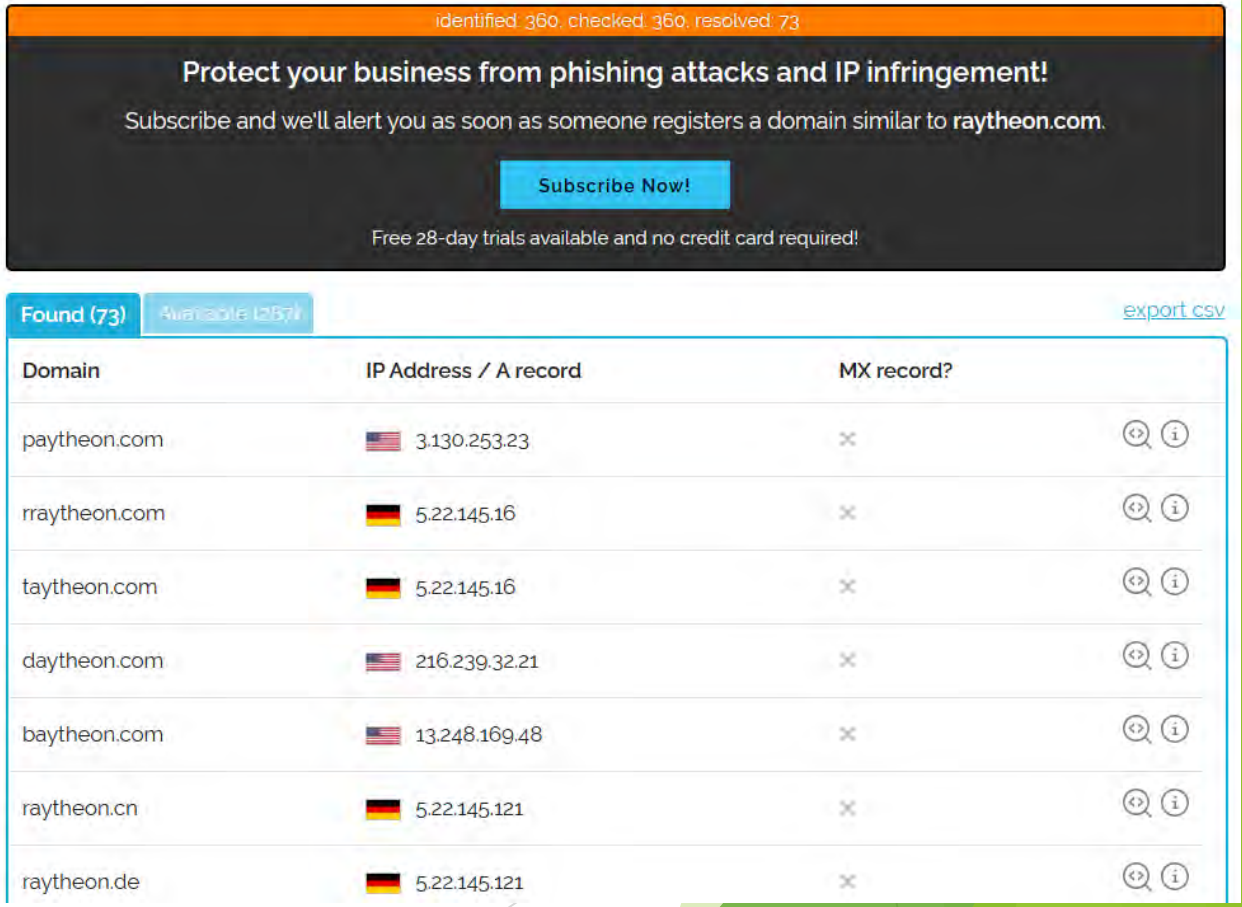
Кому

Please do not reply to this message**********

War Story/Practical Exercise



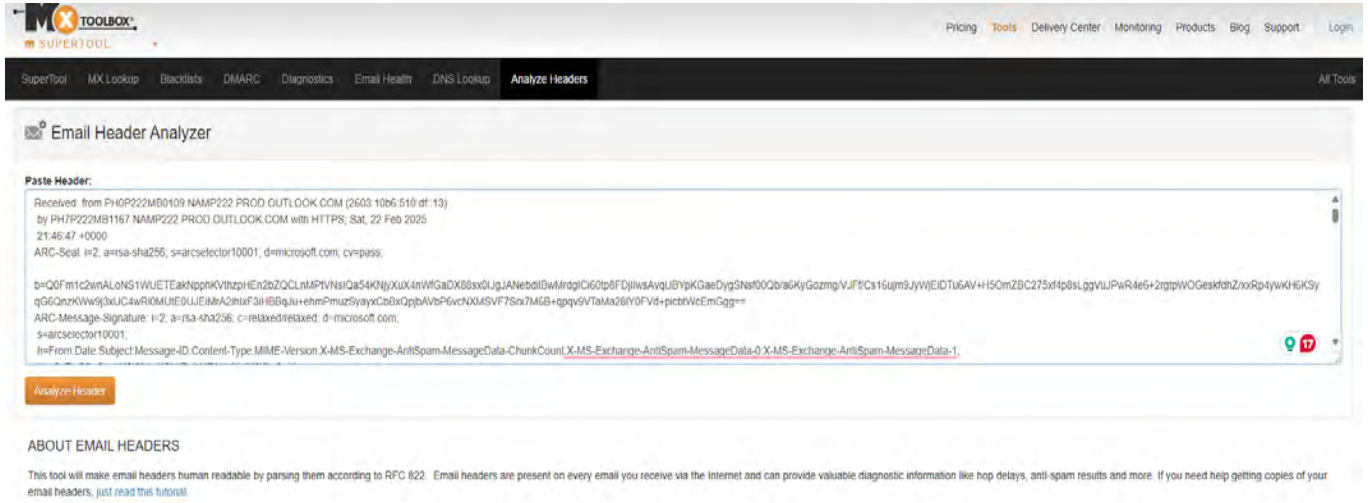
Visit:
www.dnstwister.report



Email Headers

- An email header contains technical details about the email origin and path to destination.
  - Can determine original sender email address.
  - Source IP of sender.
  - Reply-to mailbox.
  - Security configurations like DKIM, DMARC, and SPF records.

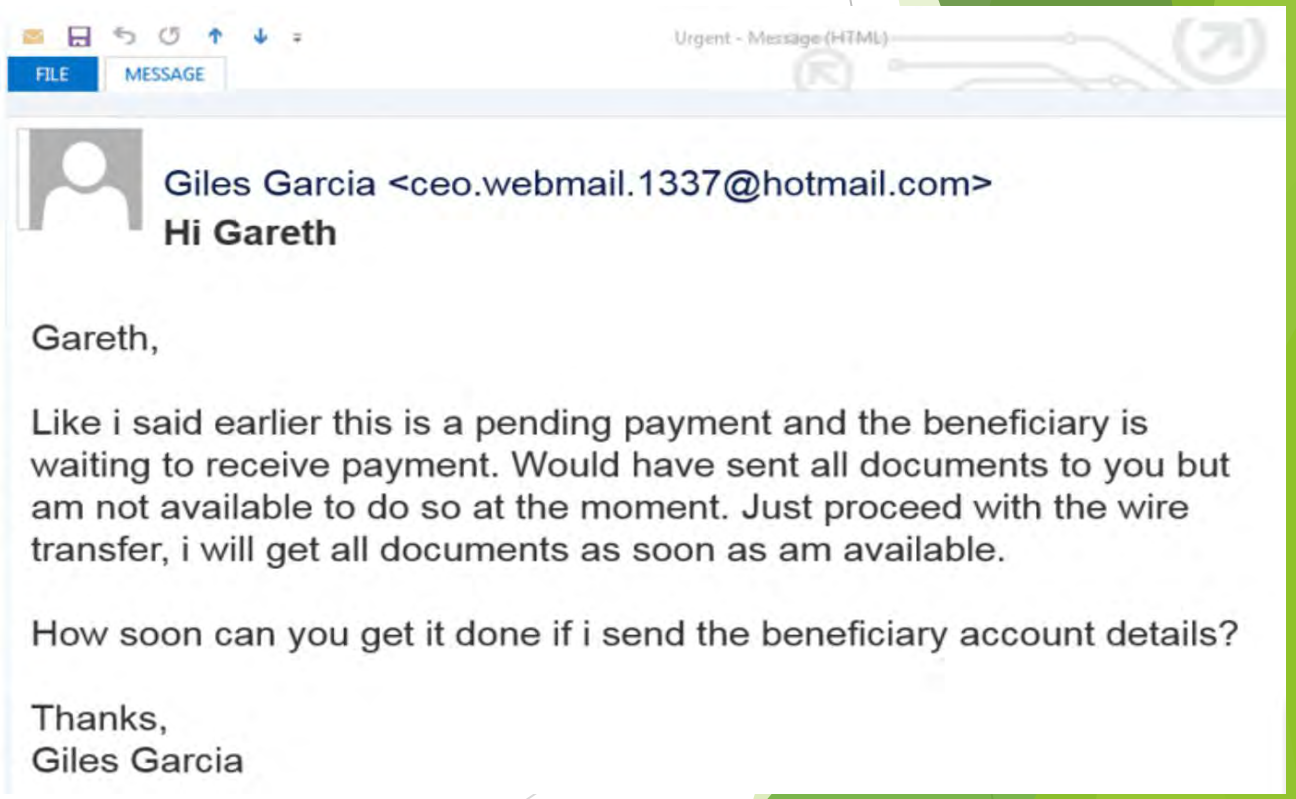
- Mx Toolbox www.mxtoolbox.com




```
X-Pm-Content-Encryption: end-to-end
X-Pm-Origin: internal
Subject: Seattle trip
To: Kristen Novak <kristennovak@proton.me>
From: Eric Norbert <eric.norbert@proton.me>
Date: Tue, 14 Mar 2023 16:29:46 +0000
Mime-Version: 1.0
Content-Type: text/html
Message-Id:
<hvllFNSqLpe7Va0W4vl8oXzhimc9lBJQLKOjSg0zJtRzWZkzfohHSH0h5yTrIXn_pQ76eZMB7EzXQG
R3Q15LGKQGec9ZNdSuLgp1rj6TUXI=@proton.me>
X-Pm-Spamscore: 0
Received: from mail.protonmail.ch by mail.protonmail.ch; Tue, 14 Mar 2023
16:29:53 +0000
X-Original-To: kristennovak@proton.me
Return-Path: <eric.norbert@proton.me>
Delivered-To: kristennovak@proton.me
```

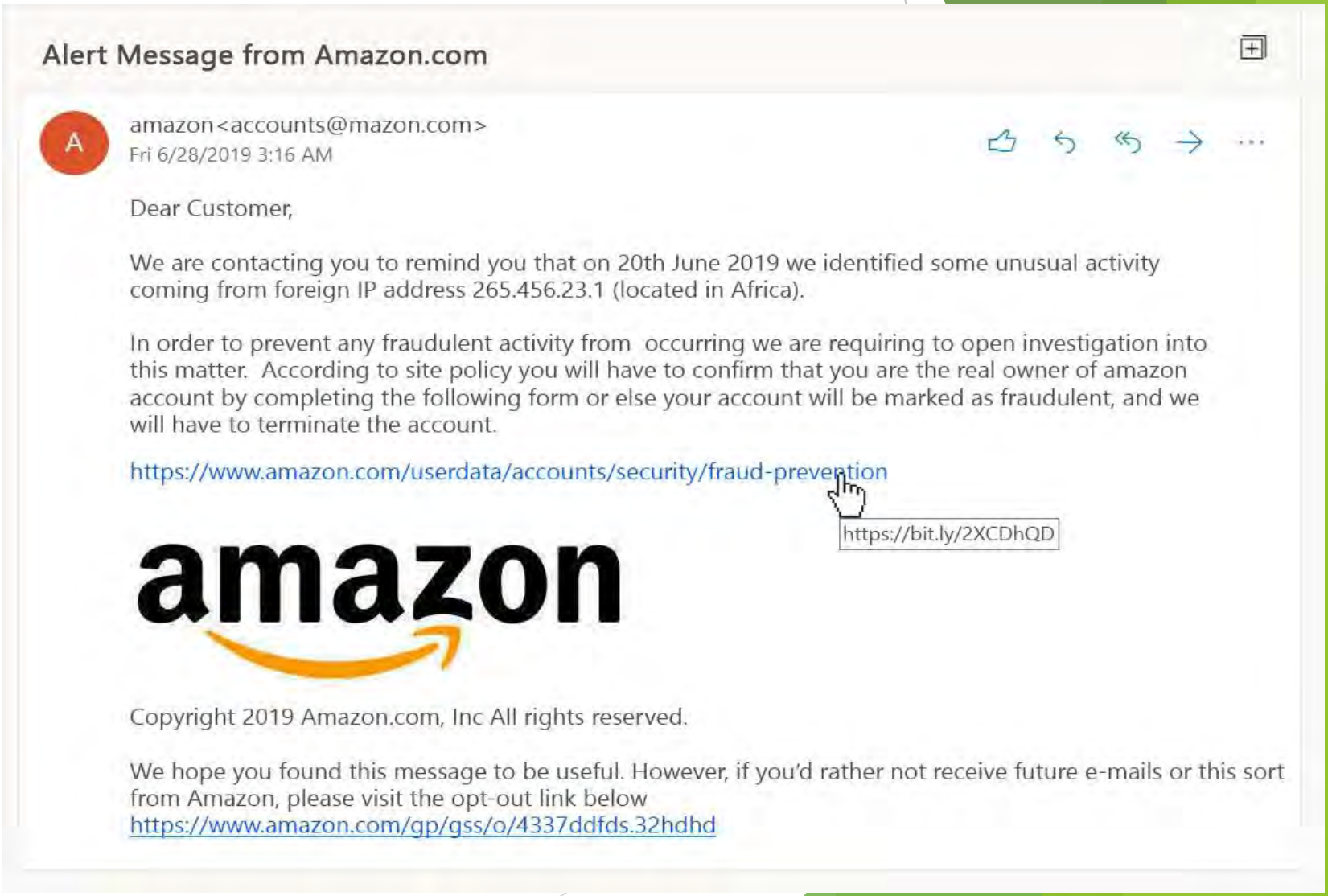
Greetings!!

- Review the greeting. This is used to establish trust; does it make sense? Is it generic/accurate?

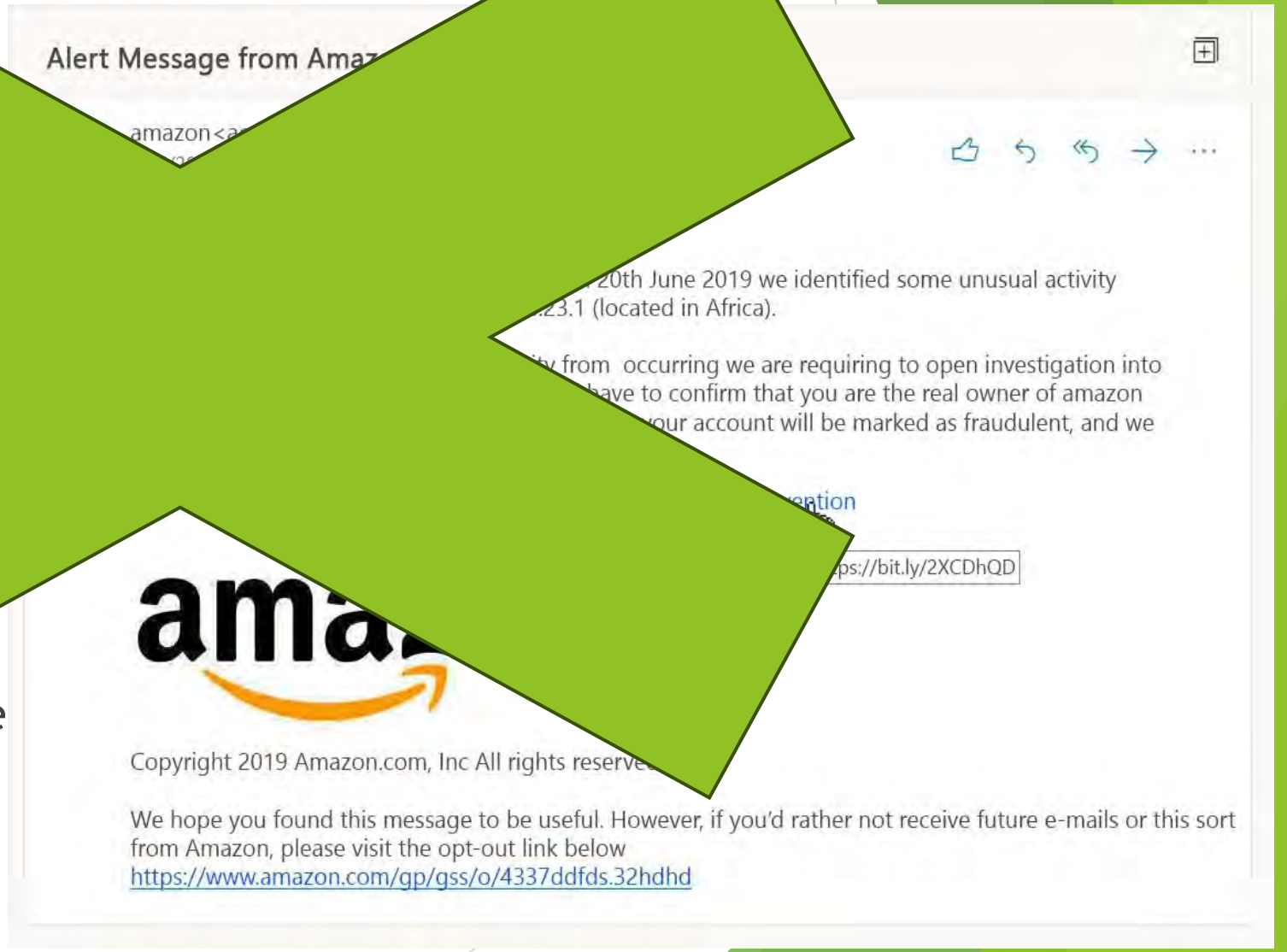


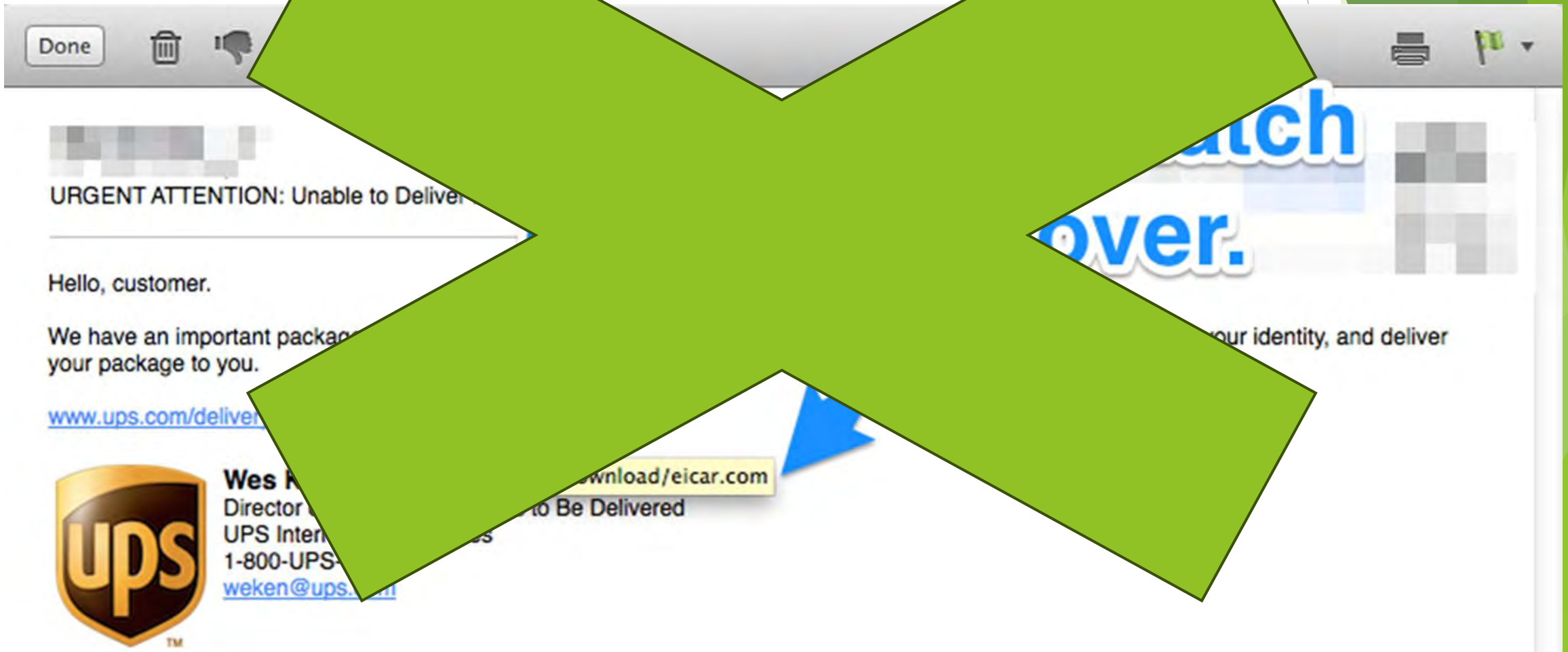
Content Analysis?

- Review the content objectively.
  - Sense of urgency
  - Negative action
  - Windfall
  - False contest
  - Established trust
  - Empathy/support



- Hover over th… the intended re…
  - Does it m…
  - Is it shorter/lon…
  - Spelled correctly
  - Out of character
- Right Click if need… CAUTIOUS
- https://unit… m/rare-phish… header-refresh/#:~:text… 42%20rese… archers%20observ… 20many

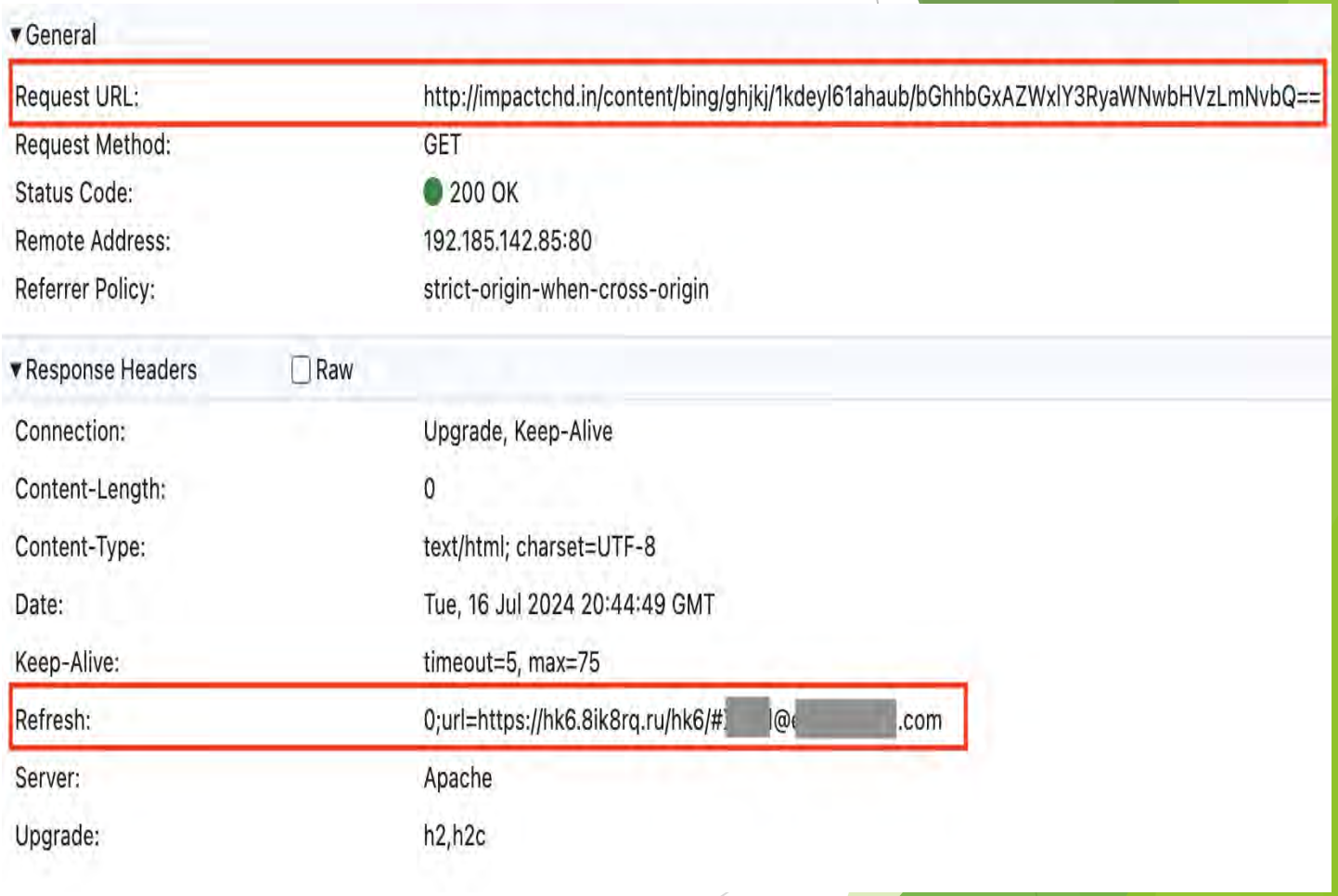



Done
URGENT ATTENTION: Unable to Deliver
Hello, customer.
We have an important packa
your package to you.
www.ups.com/deliver
Wes H
Director
UPS Inter
1-800-UPS-
weken@ups.com
ownload/eicar.com
to Be Delivered
ups
atch
over.
our identity, and deliver

Link Hovering-Header Refresh

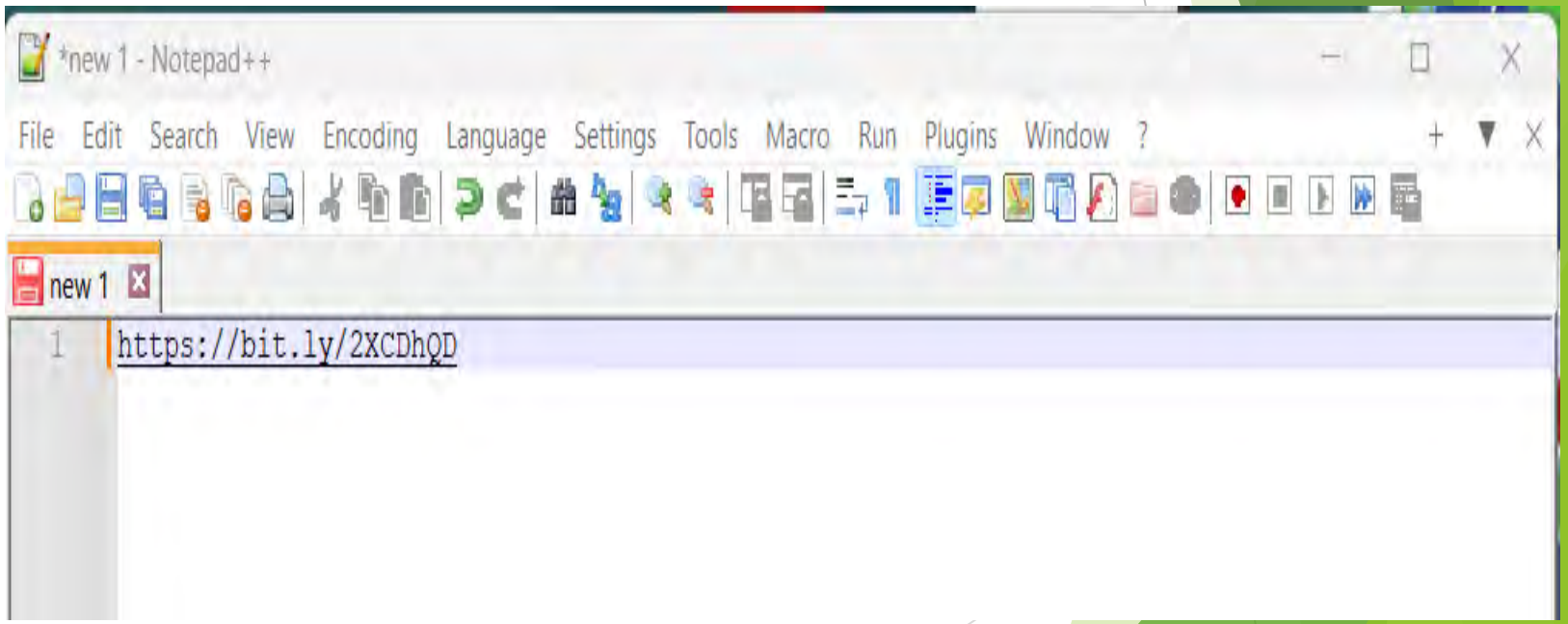
- Phishing webpage distributed through embedded links in content.
- Attackers have created a way to redirect to a different link then displayed when hovering.
- Individual is redirected to a different site containing email address for cred harvesting.

- https://unit42.paloaltonetworks.com/rare-phishing-page-delivery-header-refresh/#:~:text=Unit%2042%20researchers%20observed%20many



What Next?!

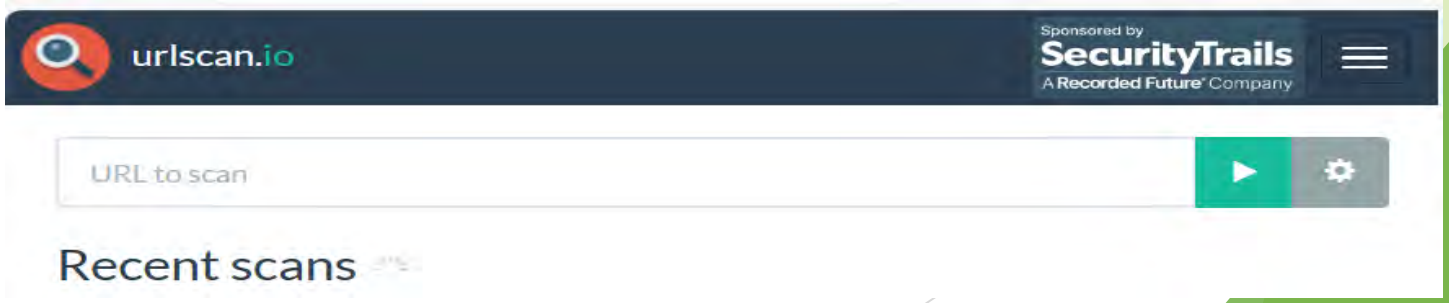
- Copy the Link, paste it in Notepad++.
- Get ready to analyze!!



The Best Link Analysis Tools

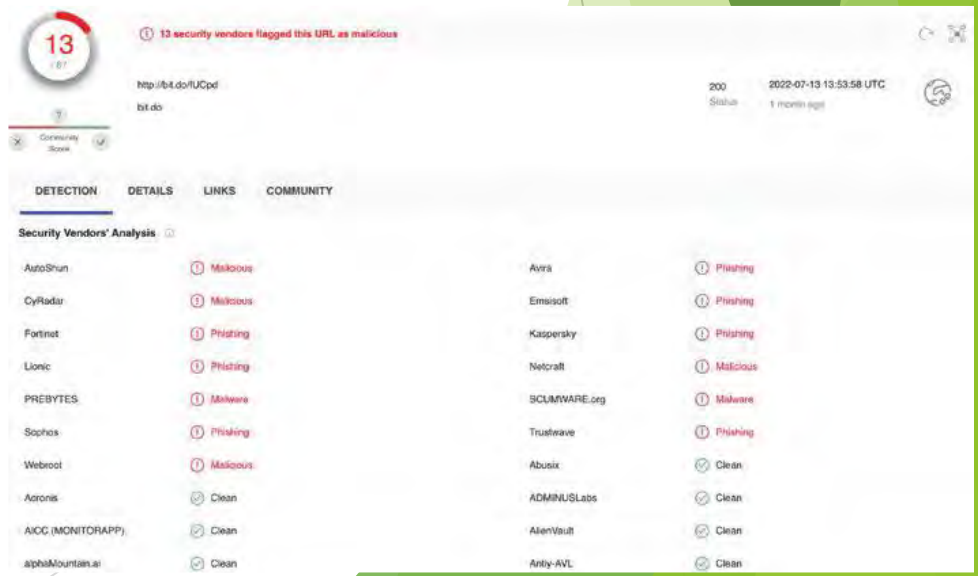
- Link analysis tools scan a provided hyperlink providing additional technical details on the validity of a resource.
  - Most check a known repository of reported malicious sites.
  - Some scan the page and make a determination.
  - Few let you interact with the page.
- Virustotal.com

- URLscan.io



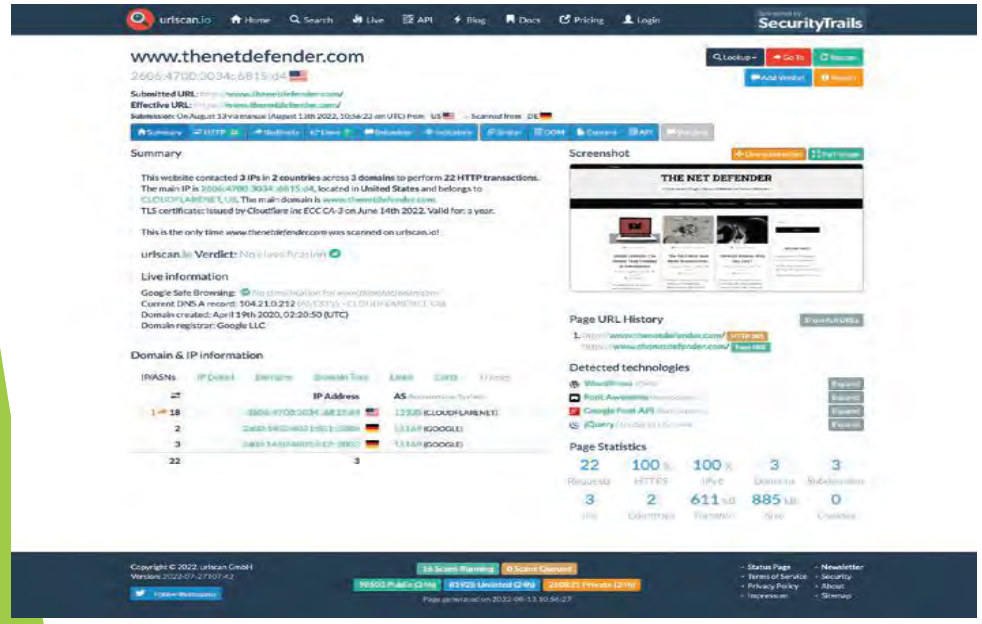
Virustotal

- Link analysis tool scans a provided hyperlink for malicious indicators.



URLscan

- Similar, ****BUT grabs a screenshot****



Practical

- www.virustotal.com
- www.urlscan.io

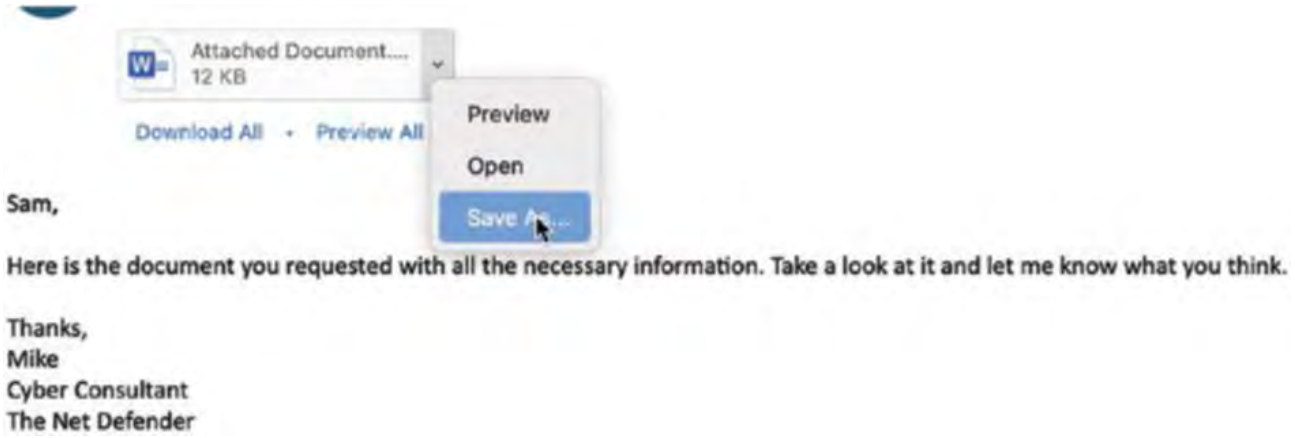
- https://tinyurl.com/8rxd5hr7
- https://tinyurl.com/5dncrxdp
- https://rb.gy/2pvfj
- https://rb.gy/nh3l4
- https://rb.gy/12drp
- https://rb.gy/1cx7n
- https://tinyurl.com/mvsmdmh8

Attachments

- Computer files sent with an email message, can contain malicious code!!!

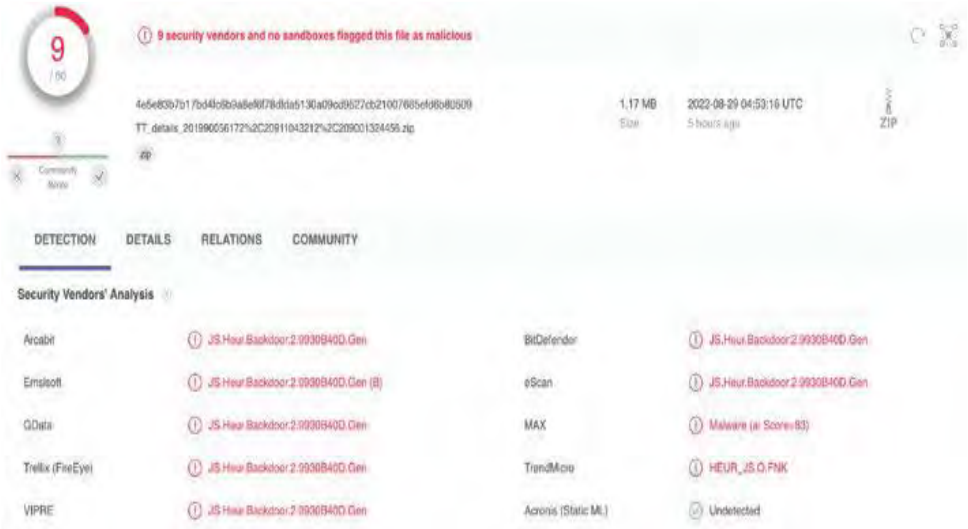
Questions to Ask?

- Does this make sense?
- Did I ask for this file?
- Do I NEED this information for my job?
- Does the attachment align with the email content?
- Should I extract this and analyze?

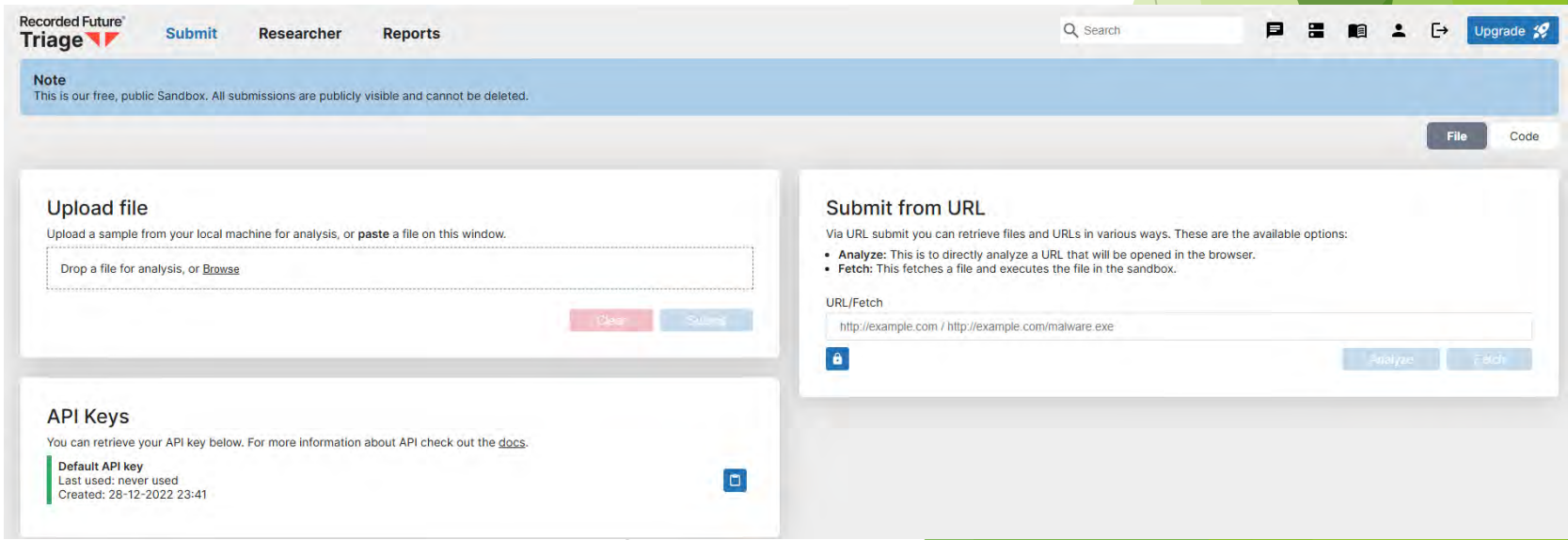


Best Attachment Tools

- VIRUSTOTAL



- Tria.ge- Triage by Recorded Future



Themed Attacks

- IRS

To: [redacted]
SPAM: You are eligible for refund

IRS

Hello [redacted],

After the last annual calculations of your fiscal activity we have determined that you are eligible for tax refund under section 501(c) (17) of the Internal Revenue Code.

Please submit the Tax Refund Request Form and allow us 3-9 days to process it.

Yours faithfully,
Internal Revenue Service
United States Department of the Treasury

Green Dot COVID-19 Benefits

Complete the following appropriately to receive your benefits.

	First Name:	Middle Name:	Last Name:
Full Name:			

Date of Birth: SSN: Sex:

Street Address: City:

State: Zip code:

Phone Number: Email Address:

Payment Option

Note: Payments will only be made/apply to a new Green Dot Prepaid Visa Card.

* Visit any green dot retailers nationwide including (7-Eleven, ACE Cash Express, CVS/Pharmacy, Dollar General, Family Dollar, Kmart, Kroger, Rite Aid, Safeway, Walgreens and Walmart) and buy any Green Dot Reloadable Visa Debit Card.

* You will complete the below section with your purchased Green Dot Reloadable Visa Debit Card details and submit along with your application.

* Do not register/activate your Green Dot Reloadable Visa Debit Card.

Card Number:

Expiring Date: MM YY

CVV/CVC:

---------- Forwarded message ----------
From: "Unemployment Advisory Department" <support@us-benefits.org>
Date: Jan 16, 2015 10:12 AM
Subject: Required Documents to File Unemployment in MO
To:
Cc:

REQUIRED DOCUMENTS AND INFORMATION TO FILE UNEMPLOYMENT IN MO

Do not apply online for unemployment benefits in City, State before collecting all the information and documentation that will be required. Because of the high number of applicants, and the time it takes to process each one, following directions is extremely important.

Important: In the next step, we're going to check all possible reasons why you might not qualify for unemployment. This is extremely important because if you file and then get denied, you will have to go through a very lengthy appeals process to correct any errors.

=> Click Here to Continue

Please understand that your chances of getting denied go up the longer you wait to submit your official application.

Don't miss any of your benefit payments. Click the link below:
=> File Unemployment Online

Support Team

Employment Advisory Department

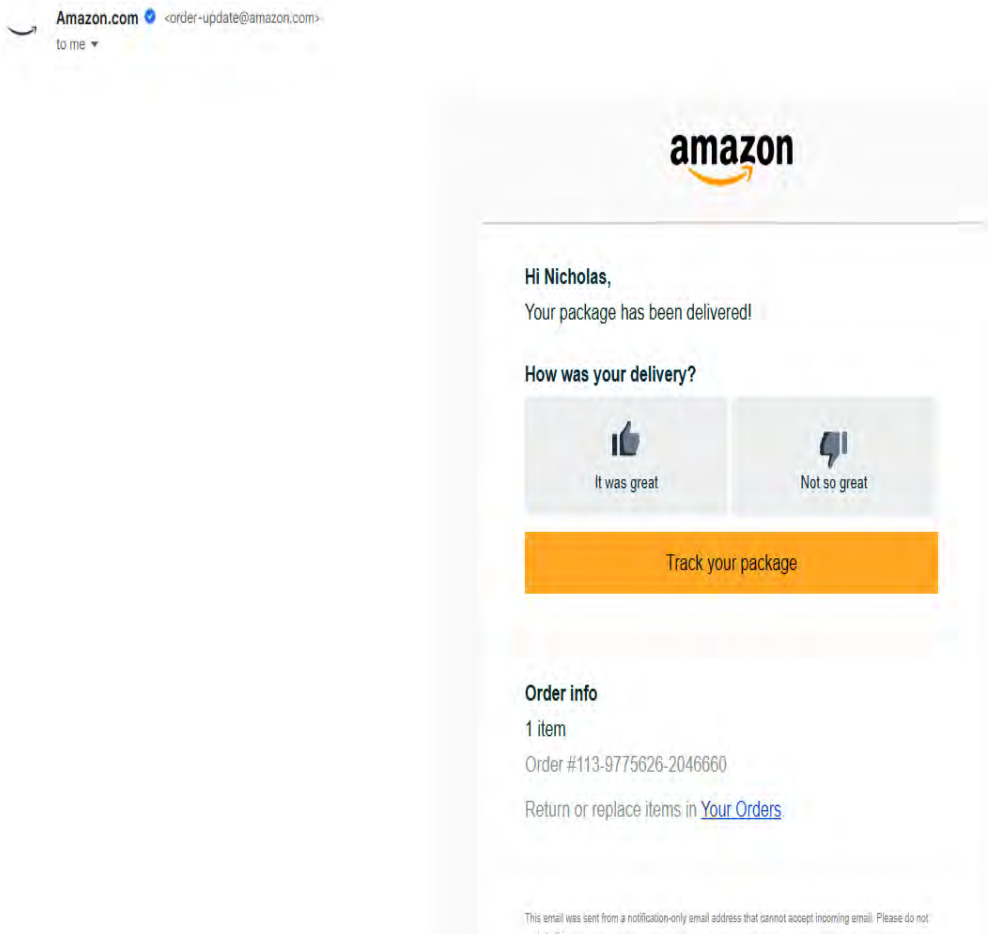
You are receiving this email because you requested information online

This message was sent to from:

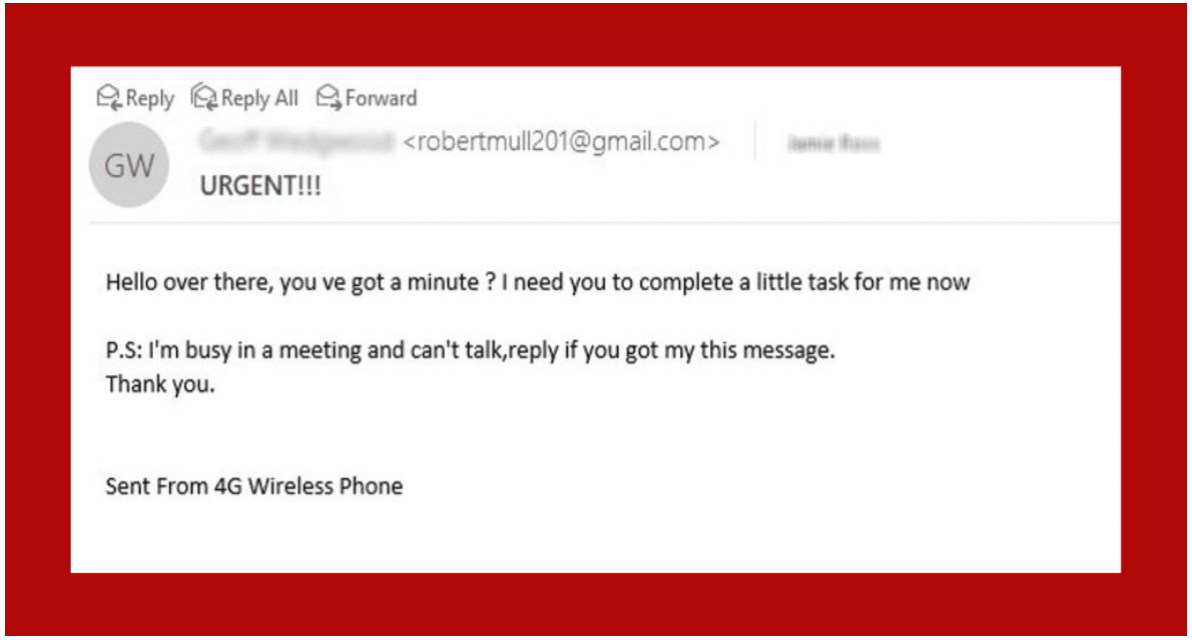
Unemployment Advisory Department | support@us-benefits.org | Employment Advisory | 123 Main Street | NYC, NY 10314

Themed Attacks

- Package Delivery



Wire Transfers/Gift Cards



Reply Reply All Forward

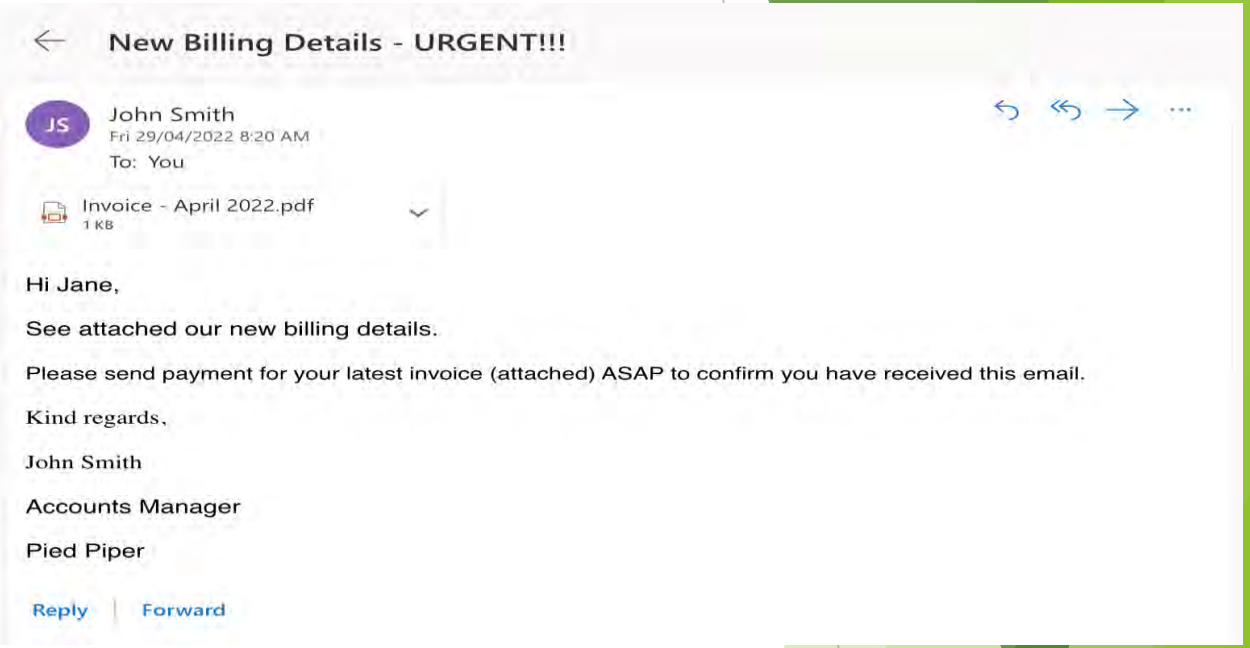
GW <robertmull201@gmail.com>

URGENT!!!

Hello over there, you ve got a minute ? I need you to complete a little task for me now

P.S: I'm busy in a meeting and can't talk,reply if you got my this message.
Thank you.

Sent From 4G Wireless Phone



New Billing Details - URGENT!!!

JS John Smith
Fri 29/04/2022 8:20 AM
To: You

Invoice - April 2022.pdf
1 KB

Hi Jane,

See attached our new billing details.

Please send payment for your latest invoice (attached) ASAP to confirm you have received this email.

Kind regards,

John Smith

Accounts Manager

Pied Piper

Reply | Forward

Urgent Favor

C CEO <ceo@spoofed.gmail.com>
To

11:35 AM

External Message

Dear X,

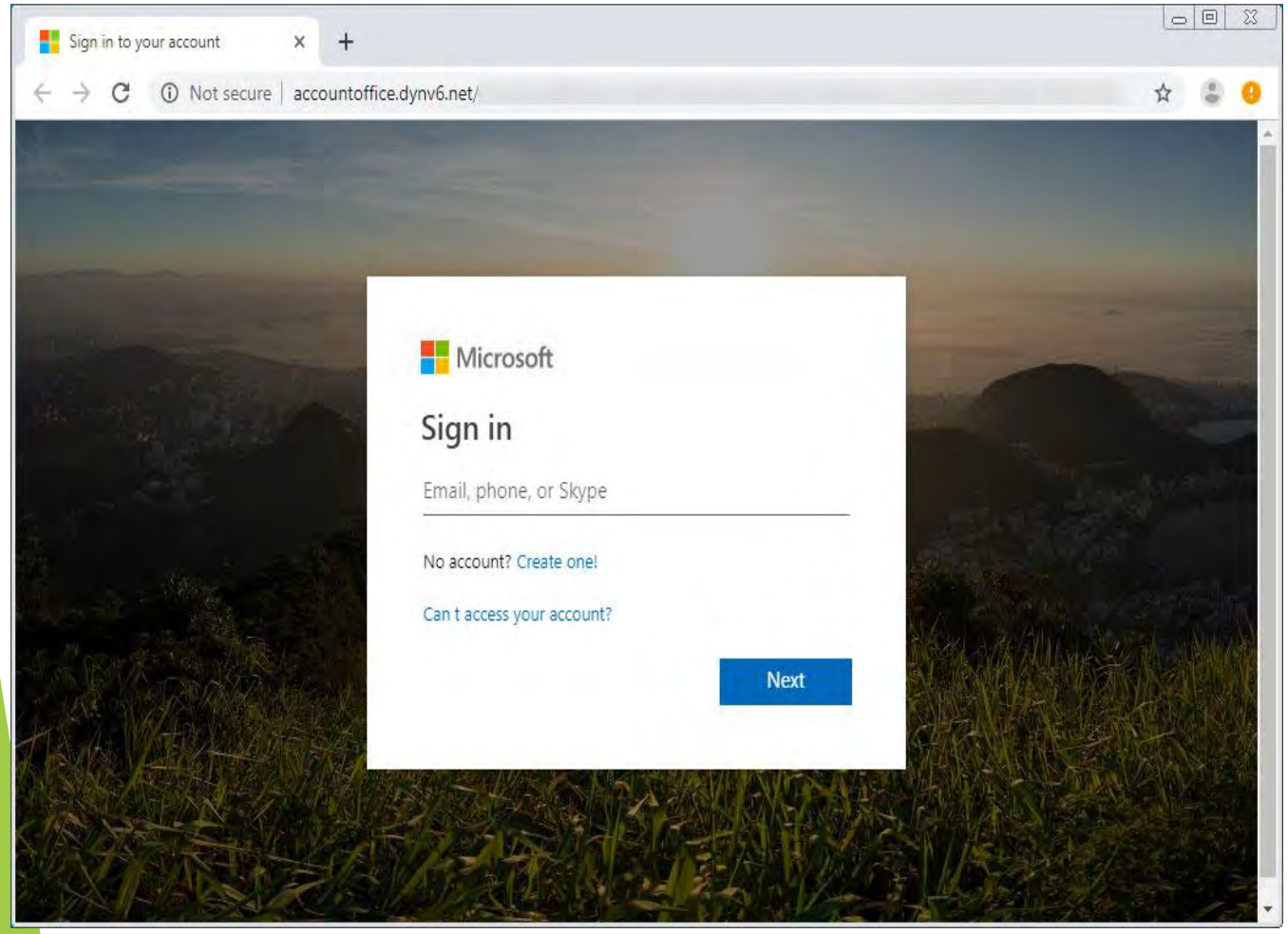
Are you available?

I need gift cards for a select group of clients and have to send them out in less than an hour. I would provide you with the type of gift cards and amount of each.

Sent from my iPad

NOTE: This email originated from outside Chapman's network. Do not click links or open attachments unless you recognize the sender and know content is safe.

Where This Leads

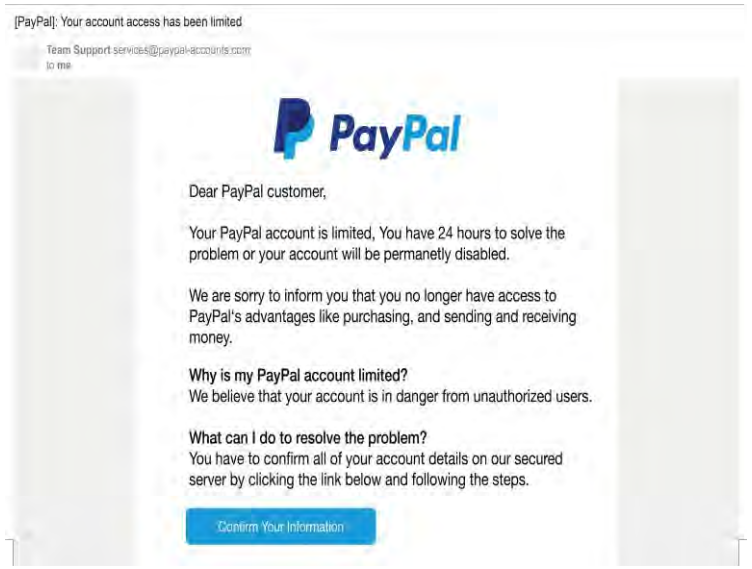


What to do?!

- Report the message!!
  - Internal security team
  - Email provider (Google, Yahoo, AOL ect)
- Share the message
  - Post on social media
  - Talk to your friends about it
- Delete the message

Fix Security Awareness 3 Things

+



+

Cyber Resources

Top Podcasts

Cyber Security Headlines (10 minutes)

Cyberwire Daily (40 minutes)

Sans Internet Storm Center (10 Minutes)

Down the Security Rabbithole (60 Minutes)

Darknet Diaries (60 minutes)

Top News Sites

Thehackernews.com

Bleepingcomputer.com

Krebsonsecurity.com

Csoonline.com

Darkreading.com

Top Publications

Verizon Data Breach Investigations Report

IBM Cost of a Data Breach

Mandiant M-Trends

Red Canary Annual Report

Top Tools

1. Virustotal.com
2. Urlscan.io
3. Tria.ge
4. Joesandbox.com
5. Alienvault.com

Top X Feeds

1. @vxunderground
2. @Troyhunt
3. @briankrebs
4. @swiftonsecurity
5. @hacks4pancakes

Top Books

1. The Cuckoo's Egg Clifford Stull
2. Dark Territory Fred Kaplan
3. Fifth Domain Richard Clarke
4. Sandworm Andy Greenburg
5. @War Shane Harris

Questions/Comments

- Entoo Security
  - FTC Safeguards
  - Penetration Tests
  - vCISO and Consulting
  - Risk Assessments
  - Incident Response
  - Security Awareness Training